BCLP. Client Intelligent

Insights

WASHINGTON MY HEALTH DATA ACT FAQ'S: PROCESSING BIOMETRIC DATA

Mar 05, 2024

WHAT ARE THE UNIQUE FEATURES CONCERNING THE PROCESSING OF BIOMETRIC DATA UNDER THE MHMDA?

The MHMDA defines “biometric data” very broadly.[1] Specifically, biometric data is “data that is generated from the measurement or technological processing of an individual’s physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data.”[2]

The definition includes by way of example a number of identifiers that are typically associated with biometric data in other, more well-known, statutes like Illinois’ BIPA—identifiers like the imagery of an iris, a retina, a fingerprint, and other traditional biometric PII. But that is not all that counts as biometric data under MHMDA. Specifically, section 3(4)(b) states that biometric data also “includes, but is not limited to . . . [k]eystroke patterns or rhythms and gait patterns or rhythms that constitute identifying information.”[3] This is a noteworthy expansion for a few reasons:

- Neither gait—that is, the distinct manner in which someone walks or moves[4]—nor keystroke patterns are typically found in other definitions of biometric data.[5] Many other statutes, including BIPA, contain broad catch-all language, but the inclusion of gait is a relative rarity.[6] Gait can, in fact, be used to identify an individual. For example, the Associated Press reported that Chinese authorities utilized such a tool in 2018.
- It is important to remember, however, that the data must also qualify as “consumer health data” to be regulated under MHMDA.[7] MHMDA is not a broad “omnibus” data privacy law. It is targeted at a specific type of PII—namely, consumer health data. But here, the MHMDA appears to be making a categorical assertion that all biometric data, including gait data, is health data.[8] The statute provides that, “for the purposes of the [definition of consumer health data], physical or mental health status, includes but is not limited to: (ix) [b]iometric data.”[9] Whether this expansive reading survives scrutiny in practice remains to be seen.
- Indeed, such an expansive reading may be especially problematic as it pertains to keystroke pattern logging. It is unclear how device fingerprinting or keystroke pattern logging which

> identifies an individual could plausibly be considered data that “identifies the consumer’s past, present, or future physical or mental health status.”[10] Yet because keystroke patterns are within the definition of “biometric data” and “biometric data” is categorically included in the examples provided of “physical or mental health status,” there is potentially an argument that all keystroke pattern logging data sufficient to identify a Washington consumer is “consumer health data” regulated by the Act.

Whether these expansive applications are ultimately adopted by regulators and courts remains to be seen. At this juncture, we can only note that the definition of biometric data under the MHMDA is quite a bit broader than that found in other laws.

FOOTNOTES

[1] *See*, MHMDA Section 3(4).

[2] *Id.*

[3] *Id.* (emphasis added).

[4] “Gait” is not defined by MHMDA. Webster’s online dictionary gives the following primary definition: “a manner of walking or moving on foot.”

[5] *See, e.g.*, RCW 19.375.010 (Washington Biometric Privacy Protection Act); 740 ILCS 14 Section 10 (Illinois Biometric Information Privacy Act); and Tex. Bus. & Com. Code Section 503.001(a) (Texas Capture or Use of Biometric Identifier Act). “Gait” and “keystroke patterns” are included under the definition of "biometric data" in NRS 598.0977 Section 5 (Nevada Consumer Health Data Privacy Law), and under the definition of “biometric information” in the CPRA Section 1798.140(c) (California Consumer Privacy Act).

[6] *See*, 740 ILCS 14 Section 10 (Illinois Biometric Information Privacy Act) ("biometric information"); *see also*, RCW 19.375.010 (Washington Biometric Privacy Protection Act) ("biometric identifier"); CTDPA Section 1(4) (Connecticut Data Privacy Act); DPDPA Section 12D-102(3) (Delaware Personal Data Privacy Act); FDBR Section 5(4) (Florida Digital Bill of Rights); ICDPASection 1.2(4) (Indiana Consumer Data Protection Act); ICDPA Section 715D.1(4) (Iowa Consumer Data Protection Act); MTCDPASection 2(3) (Montana Consumer Data Protection Act); New Jersey Privacy Law Section 1; OCPA Section 1(3) (Oregon Consumer Privacy Act); TIPA Section 47-18-3201(3) (Tennessee Information Protection Act); TDPSA Section 541.001(3) (Texas Data Privacy and Security Act); UCPA Section 13-61-101(6) (Utah Consumer Privacy Act); and VCDPA Section 59.1-575 (Virginia Consumer Data Privacy Act).

[7] MHMDA Section 3(8)(b)(ix) (listing biometric data as a type of consumer health data).

[8] *Id.*

[9] *Id.*

[10] *Id.* at 3(8)(a) (defining consumer health data).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Lauren J. Caisman

Chicago

lauren.caisman@bclplaw.com
+1 312 602 5079

Annalisa Kolb

Chicago

annalisa.kolb@bclplaw.com
+1 312 602 5062
